



(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention
of the grant of the patent:
02.11.2005 Bulletin 2005/44

(51) Int Cl.⁷: **G07C 9/00**

(21) Application number: **98123757.1**

(22) Date of filing: **14.12.1998**

(54) **Remote authentication system**

Fernbeglaubigungssystem

Système d'authentification à distance

(84) Designated Contracting States:
DE FR GB

(30) Priority: **05.02.1998 JP 2422598**

(43) Date of publication of application:
11.08.1999 Bulletin 1999/32

(73) Proprietor: **MITSUBISHI DENKI KABUSHIKI
KAISHA
Tokyo 100-8310 (JP)**

(72) Inventors:
• **Nakamura, Hiroshi**
Chiyoda-ku, Tokyo 100-8310 (JP)
• **Fujii, Teruko**
Chiyoda-ku, Tokyo 100-8310 (JP)

• **Sadakane, Tetsuo**
Chiyoda-ku, Tokyo 100-8310 (JP)
• **Baba, Yoshimasa**
Chiyoda-ku, Tokyo 100-8310 (JP)

(74) Representative: **Pfenning, Meinig & Partner GbR**
Mozartstrasse 17
80336 München (DE)

(56) References cited:
EP-A- 0 762 261 **WO-A-97/15007**
WO-A-98/10412 **WO-A-98/57247**
GB-A- 2 204 971

• **PATENT ABSTRACTS OF JAPAN vol. 1997, no.**
04, 30 April 1997 (1997-04-30) & JP 08 329010 A
(TOSHIBA CORP), 13 December 1996
(1996-12-13)

Note: Within nine months from the publication of the mention of the grant of the European patent, any person may give notice to the European Patent Office of opposition to the European patent granted. Notice of opposition shall be filed in a written reasoned statement. It shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

Description

BACKGROUND OF THE INVENTION

1. Field of the Invention

[0001] The present invention relates to a remote authentication system in which identification of an individual by biometrics and decision of presence or absence of access right to the information of the individual and application are made intensively by a single authentication terminal.

2. Description of the Related Art

[0002] Conventionally, in an information processing system connected to a network, for security, an operation of identifying an individual to decide access permission and inhibition of the individual, i.e., authentication is required. Further, an automatic teller machine of a bank or the like generally carries out authentication for identification of an individual and accessing to transaction information of the individual such as balance of the deposit. Authentication of an individual is also carried out for arrival or departure to a research place with high security and member's club.

[0003] The authentication, i.e. identification of an individual and recognition of qualification, is carried out using a magnetic card or IC card which has the same function as an ID card, individual's memory such as a password or a combination thereof. However, the password may be forgotten. It may happen that the magnetic card or IC card cannot be authenticated because of losing or breakage. The individual other than a person in question may be authenticated as the person in question because of steal of the card or leakage of the information of the password. In order to keep high security, the person in question must be surely authenticated as himself or herself. In this case, if the means of complicating the password or one-time password (OTP) is adopted, memorizing is difficult correspondingly, or the operation of authentication itself becomes complicate. Further, if authentication by memory is executed in a wide area (plural stores of the bank), authentication information must be managed intensively.

[0004] On the other hand, authentication by biometrics information, which represents living-body characteristics of an individual such as information relative to a fingerprint, a handprint, handwriting, retina, etc. removes the complication and also makes "posing" difficult. If the authentication by biometrics information is required in a wide region, intensive management and authentication are required for the same reason and protection of privacy. When the authentication by biometrics information is executed intensively, it is important to select a suitable method of authentication according to a security level such as a matter, place or system requiring authentication as well as each user, thereby acquiring

ing the authentication information.

[0005] Now, the RADIUS server, which is described by RFC 2138 (Remote Authentication Dial In User Service, hereinafter referred to as RADIUS, renewal of the previous RFC 2058) which is registered in RFC (Request For Comment) of IETF (Internet Engineering Task Force), in response to a request from a RADIUS client, performs the authentication processing intensively to send back the result of authentication. In this case, the authentication means and authentication information are fixedly defined for each user. For this reason, if the biometrics information is to be acquired, according to its acquisition environment, the authentication means and authentication information cannot be changed dynamically.

[0006] One example of such a prior art is an "authentication method on a network" disclosed in JP-A-9-81518. In this method, when a user host accesses to an application server, the application server requests an authentication server to make authentication of a user using fixed authentication means and authentication information and receives the result of authentication.

[0007] The biometrics information is efficient to discriminate an individual from other persons. However, it gives rise to problems of privacy protection and sanitary acquisition when a biometrics acquisition device itself involves dirtiness and unpleasantness.

[0008] US-A-4 993 068 discloses an unforgeable personal identification system for identifying users at remote access control sites. The unforgeable personal identification system generates one-way encrypted versions of physically immutable identification credentials (facial photo, retinal scan, voice and finger prints). These credentials are stored on a portable memory device. At a remote access control site, the user presents his portable memory device and the encrypted identification credentials are read. The user then submits physically to inputting of his physical identification characteristics to the remote access control site. Comparison is performed with the credentials obtained from the memory device and with the user's physical identity to determine whether to allow or deny access at the remote site. The credentials can be used singly or in combination for comparison with the user's physical identity. Further, attribute or privilege information can be added to the credentials and coupled with the immutable physical trails. Such data may include medical information about the user, particular privileges held by the user, such as organizational affiliations, security clearance levels, passport and visa information or financial information.

SUMMARY OF THE INVENTION

[0009] The present invention has been accomplished to solve the problem as described above, and intends to provide a remote authentication system and remote authentication method which can surely identify an individual and decide the presence or absence of an access

right thereof when the individual is authenticated using biometrics information and also can improve ease of usage.

[0010] This object according to the invention is solved by a remote authentication system comprising the features of claim 1.

[0011] The present invention provides a remote authentication system having a network which is connected to an authentication server, an authentication client and a user terminal for accessing data from the authentication client, in which authentication of the user accessing the authentication client is made through the user terminal, comprising plural kinds of biometrics acquisition devices connected to the user terminal, and plural authentication information acquisition software's stored in said authentication server according to the user terminal and/or a user, wherein in accordance with the operation of a prescribed authentication acquisition software corresponding to the user terminal, which is downloaded from the authentication server in authentication, biometrics information acquired by one or plural kinds of biometrics acquisition devices and/or keyed-in user discrimination information are used which are selected depending on the secret level of the data to be accessed.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012]

Fig. 1 is a block diagram of the first embodiment of a Web system to which the remote authentication system according to the present invention is applied.

Fig. 2 is a timing chart for explaining processing of authentication in the Web system in Fig. 2.

Fig. 3 is a graph for explaining a first example of an authentication information database in the authentication server terminal in Fig. 1.

Fig. 4 is a graph for explaining a first example of an authentication information database in the authentication server terminal in Fig. 1.

Fig. 5 is a graph for explaining a second example of an authentication information database in the authentication server terminal in Fig. 1.

Fig. 6 is a graph for explaining a third example of an authentication information database in the authentication server terminal in Fig. 1.

Fig. 7 is a graph for explaining a third example of an authentication information database in the authentication server terminal in Fig. 1.

Fig. 8 is a timing chart for explaining the authentication processing of the third example in the Web system shown in Fig. 1.

Fig. 9 is a block diagram of the second embodiment of the Web system to which a remote authentication system according to the present invention is applied.

Fig. 10 is a timing chart for explaining the authentication processing in the Web system shown in Fig. 9.

Fig. 11 is a timing chart for explaining the case where rejection occurs as the third embodiment of the Web system in Fig. 1.

Fig. 12 is a schematic view of the fourth embodiment of the Web system in Fig. 1.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0013] Now referring to the drawings, an explanation will be given of embodiments of the present invention.

Embodiment 1

[0014] Fig. 1 shows a configuration of the first embodiment when the present invention is applied to a Web system. A network 2 is connected to an authentication server terminal 3, an authentication client terminal 4 (Web server terminal in this embodiment) and a user terminal 5, etc. In such a Web system 1, the Web server 4, when it is accessed through the user terminal 5 from a user, receives individual authentication of the user from the authentication server terminal 3, and on the basis of the result, provides service to the user.

[0015] The authentication server terminal 3 is a computer device such as a personal computer, workstation, etc. (which may include a CPU, memory, disk, communication control unit, etc. as described hereinafter) which stores an authentication control unit 3A, authentication information data base 3B and authentication information acquisition software pool 3C (hereinafter, software will be referred to S/W). The Web server terminal 4 is a computer device such as a personal computer, workstation, etc. in which a Web server data base 4A, authentication request unit 4B and a Web server S/W 4C requiring authentication of a user are operated.

[0016] The user terminal device 5 is composed of a browser for displaying information of the Web server terminal 4 and a computer device such as a personal computer or workstation in which authentication information acquisition S/W 5B are operated. The user terminal device 5 is connected to a biometrics acquisition device 6. The biometrics acquisition device 6 includes a fingerprint acquisition device 7 and a handprint acquisition device 8 which acquire a fingerprint and handprint of a living body as biometrics information, respectively, through image processing, a letter recognition tablet 9 for acquiring handwriting information written by a user as biometrics information, a retina information acquisition device 10 for acquiring retina information of a living body as biometrics information by scanning of an eye-ground.

[0017] A processing flow of authentication in such a Web system is shown in Fig. 2. First, an explanation will be given of the case where a user accesses the infor-

mation of the Web server data base 4A with a high secret degree in the Web server terminal 4 which is a client of authentication, using the browser 5A which is an application operating in the user terminal device 5 (SP1). The Web server S/W 4C which is an application making access control of the information with a high secret degree must make user authentication in order to decide whether the user has an access right (SP10).

[0018] Namely, the Web server S/W 4C in the Web server terminal 4 informs the authentication request unit 4B of necessity of the user authentication as well as a client ID (identifier of the authentication request unit), an application ID (identifier of the Web server S/W 4C which is an application requiring authentication) and an access data class (secret level of the data accessed by the user) (SP11). The authentication request unit 4B transmits the authentication request of the user inclusive of the above information to the authentication server terminal 3.

[0019] The authentication control unit 3A in the authentication server terminal 3 which has received the authentication request from the user selects an authentication information acquisition S/W 11 from the authentication client ID, application ID and access data type (SP20). The authentication information acquisition S/W 11 acquires a predetermined item of information. It may acquire a plurality of items of authentication information. The authentication control unit 3A transfers the selected authentication information acquisition S/W 11 to the Web server terminal 4 which is a client of authentication (SP21).

[0020] The authentication request unit 4B in the Web server terminal 4 delivers the transferred authentication information acquisition S/W 11 to the Web server S/W 4C, instructs it to acquire the authentication information from the user. On the basis of this instruction, the authentication information acquisition S/W 11 is transferred from the Web server S/W 4C to the user terminal 5 (SP12).

[0021] The browser 5A in the user terminal 5 receives the transferred authentication information acquisition S/W 11 and operates it as an authentication information S/W 5B (SP2). The authentication information S/W 5B spontaneously acquires a user ID (name, firm, member number, address, belonging, telephone number, or ID allotted for an individual by the system), biometrics information such as information relative to a fingerprint, a handprint, handwriting, retina, and authentication information which is used normally in a conventional computer system, such as a password, one-time password, etc. In this case, it may operate in cooperation with the other S/W such as a driver acquiring the authentication information. The authentication information acquisition S/W 5B transfers the acquired user ID and authentication information to the Web server terminal 4 through the browser 5A (SP3).

[0022] The authentication request unit 4B in the Web server terminal 4 transfers the user ID and authentication

information acquired from the user to the authentication server terminal 3 through the Web server S/W 4C (SP13). The authentication control unit 3A in the authentication server terminal 3 executes the user authentication using the transferred user ID and authentication information (SP22). The authentication information such as the transferred biometrics information is checked against the individual information initially stored in the authentication information database 3B in the authentication server terminal 3. If a decision of being a person in question is made as results of checking all items of transferred authentication information, the result is informed of the Web server terminal which is a client of identification. If at least one of the results of checking is not right, a decision of not being a person in question is made. This is informed of the Web server terminal (SP23).

[0023] The authentication request unit 4B in the Web server terminal 4 having received the result of authentication, which is a client of authentication, informs the Web server S/W 4C of the result of authentication. On the basis of the result of authentication, the Web server S/W 4C decides permission or inhibition of access to the information with a high secret degree in the Web server data base 4A for the user (SP14). For example, the operation for user access such as displaying the secret information is done.

[0024] Additionally, encryption between the user terminal 5 (authentication information acquisition S/W 5B) and Web server terminal 4 and between the Web server terminal 4 and authentication server terminal 3 (authentication control unit 3A) permits the authentication information to be concealed and a menace of posing to be reduced. Likewise, encryption between the user terminal 5 (authentication information acquisition S/W 5B) and authentication server terminal 3 (authentication control unit 3A), but not between the individual terminals, also permits a menace of posing to be reduced.

Example 1

[0025] Referring to Figs. 3 and 4, an explanation will be given of a simple example of the database structure and selection processing of the authentication information acquisition S/W 5B. The authentication information database 3B in Fig. 3 includes items of user ID, user level and authentication as information allotted to an individual user. The user ID includes a name, firm, member number, address, belonging, telephone number, or any matter allotted for an individual by the system. The user level represents an access level to secret information. The authentication information is biometrics information such as information relative to a fingerprint, a handprint, handwriting, retina, and authentication information such as a password, one-time password, etc.

[0026] As seen from Fig. 4, the authentication information acquisition S/W pool stores authentication information acquisition S/Ws 11 of acquiring information of

both fingerprint and retina; acquiring fingerprint information of two fingers and acquiring information of both fingerprint and retina, etc. The authentication information acquisition S/W pool 3C describes the selectable authentication information acquisition S/W 11 corresponding to secret levels and data class.

[0027] Taking as an example the case where a user accesses the information of the Web server database 4 of the data class of 17, an explanation will be given of a mechanism of selecting the authentication information acquisition S/W 11 in the authentication server terminal 3. In this case, the authentication client ID corresponding to an identifier of the authentication request unit 4B is set at 15, and the application ID corresponding to the identifier of the Web server S/W 4C is set at 25. When access to the data class of 17 occurs, the Web server S/W 4C informs the authentication request unit 4B of necessity of user authentication. The user request unit 4B transmits the authentication request of the user, inclusive of the above items of information of the data class of 17, authentication client ID of 15 and application ID of 25, to the authentication server terminal 3. In response to this, the authentication server terminal 3 receives the authentication request inclusive of these items of information.

[0028] The authentication control unit 3A in the authentication server terminal 3 notices a selectable candidate of the authentication information acquisition S/W 11 not lower than level 2 on the basis of the database in the authentication information acquisition S/W pool 3C in Fig. 4 and that the data class due to the authentication request is level 2.

Example 2

[0029] Referring to Figs. 5 and 6, an explanation will be given of another embodiment of a part of the authentication information database corresponding to that shown in Fig. 3. These figures describe the selectable authentication information acquisition S/Ws 11 for each authentication client ID and for each application ID, respectively. The authentication control unit 3A in the authentication server terminal 3 notices candidates of the authentication information acquisition S/Ws 11 selectable from the authentication client ID and from the application ID. Therefore, on the basis of the data class, A, B, C, D, E, F are selected as candidates; on the authentication client ID, C, D, and E are selected as candidates; and on the basis of the application ID, A, D, E, and E are selected as candidates. Finally, either D or E will be selected.

[0030] The S/W selected at random or fixedly defined from candidates of the selectable authentication information acquisition S/Ws by the authentication server terminal 3 is selected by means of normal selection or sequential selection. In this embodiment, the authentication means and authentication information can be flexibly selected according to the environment such as

the data class which is access information, authentication request unit 4B operating in a device which is a client of authentication and Web server S/W 4C which is an using application. Thus, identification of an individual and decision on presence or absence of the access right of the individual can be surely made according to the environment.

Example 3

[0031] An explanation will be given of the case where an user ID is included in an authentication request and the authentication information data base shown in Fig. 3 is set in detail as shown in Fig. 7. The flow of processing in this embodiment is shown in Fig. 8 in which like reference numerals refer to like parts in Fig. 2. First, the Web server terminal 4 acquires a user ID (name, firm, member number, address, belonging, telephone number, or ID allotted for an individual by the system), and requests the authentication request unit 4B to make authentication of the user with the acquired user ID, client ID (identifier of the authentication request unit 4B), application ID (identifier of the Web server S/W 4C which is an application requiring authentication) and access data class (secret level of the data accessed by the user).

[0032] The authentication information database shown in Fig. 7, in addition to that shown in Fig. 3, includes information allotted for an individual such as a type of the user (data manager or general user), usable authentication client ID, usable application ID, application control information which is delivered to an application when authentication of being a person in question is made, and checking logs (past selection status of the authentication information acquisition S/W to the prescribed number of authentication and checking rate), total number of times of authentication, selection condition, etc.

[0033] Where the authentication request includes the user ID, the authentication information acquisition S/W will be selected in accordance with the selection condition for the user in question. For example, if the user ID is 1, and the other conditions are the same in the previous example (i.e., data class = 17, authentication client ID = 15 and application ID = 25), the authentication request unit 4B transmits, to the authentication server terminal 3, the authentication request of user as the above information inclusive of the user ID = 1, data class = 17, authentication client ID = 15 and application ID = 25.

[0034] The authentication server terminal 3 receives the request of authentication inclusive of the above information. Like the above embodiment, on the basis of the data class, A, B, C, D, E, F are selected as candidates; on the authentication client ID, C, D, and E are selected as candidates; and on the basis of the application ID, A, D, E, and E are selected as candidates. Finally, either D or E will be selected. Further, the user ID = 1, the authentication control unit 3A executes the se-

lection in the total number of times of authentication. Selection will be made in such a fashion that the first selection is D, second is E, third is E, forth is E, Now, in the total number of times of authentication is 20 with the user ID = 1, this time is 21th. Therefore, D of the authentication information acquisition S/W 11 will be selected. Other Examples

[0035] Further, as shown in Fig. 7, in the authentication information database 3B, if the authentication client ID and application ID which are usable for each user are designated, access control such as sending the authentication information acquisition S/W 11 to user only if the designated authentication client ID and application ID are designated can be realized. Now, since the usable client ID includes 15, and the usable application IS includes 25, sending of the authentication information acquisition S/W 11 is permitted.

[0036] Permission or inhibition of the authentication information acquisition S/W 11 can be decided on the basis of the user type shown in Fig. 7. Like to the user, if a secret level is allotted for the authentication client and application, the authentication server terminal 3 can select the authentication information acquisition S/W 11 on the basis of the levels of the authentication client, application and access data class. For example, control of selecting the authentication information S/W with the highest level in three levels or higher can be made.

[0037] The processing after sending the authentication information acquisition S/W 11 is different from the example described above in that only the authentication information is sent because the user ID has been acquired. Further, using Key = 1 which is control information which is delivered to the application when authentication of the person in question is Fig. 7 is made, the Web server terminal 4 can realize a variety of access controls.

[0038] In the above example, the total number of times of authentication as an example of the checking rate in Fig. 7 was used as the selection condition. In place of it, if the checking evaluation is used as the selection condition, of the authentication information acquisition S/Ws 11 with the level of 2 or higher, the one with the highest checking evaluation in the past is looked for from the checking logs of the user and selected. Now, E which has the highest checking evaluation at the last time is selected.

[0039] There is also an example of omitting the transfer of the authentication acquisition S/W from the authentication server 3 to the authentication client. Namely, where the authentication information acquisition S/W is determined fixedly by the Web server terminal which is an authentication client in the case of the Web system 1 as described above, the authentication acquisition S/W 11 previously acquired by the Web server terminal 4 may be transferred from the authentication server terminal 3 to the Web server terminal 4 without transferring the authentication information acquisition S/W.

[0040] As described above, where the authentication

is executed using the biometrics information in the Web system 1, the authentication information acquisition S/W which dynamically acquires the information required for authentication is selected in accordance with the environment (user having made access, data class which is access information, authentication request unit 4B operating in the Web server terminal 4 which is a client of authentication, Web server S/W 4C which is an using application, etc.) and authentication history (i.e. status at the time of authentication). In this way, identification of an individual and decision of the presence or absence of the access right of the individual can be surely made according to the environment.

Embodiment 2

[0041] The second embodiment of the present invention is a simplification of the first embodiment. In Fig. 9 in which like reference numerals refer to like parts in Fig. 1, the user terminal which acquires the biometrics information is the same as the terminal of the authentication client. An example of an application requiring authentication is an database retrieval application 5E for executing the database retrieval. The user terminal 5 includes a local database 5C which is used by the database retrieval application 5E, authentication request unit 5D, and a computer (personal computer or workstation) in which the database retrieval application 5E and authentication information acquisition S/W 11 are operated. The biometrics acquisition device 6 is connected to the user terminal 6, and has entirely the same configuration as that in the first embodiment. The authentication server terminal 3 has entirely the same configuration as that in the first embodiment.

[0042] An explanation will be given of the operation of the remote authentication system according to the second embodiment of the present invention. In Fig. 10 in which like reference numerals refer to like parts in Figs. 2 and 8, the database application retrieval application 5E, when it accesses the secret information in the local database 5C (SP5), first acquires a user ID (name, firm, member number, address, belonging, telephone number, or ID allotted for an individual by the system) (SP6), and requests the authentication request unit 5D to make authentication of the user with the acquired user ID, client ID (identifier of the authentication request unit 5D), application ID (identifier of the database retrieval application 5E which is an application requiring authentication) and access data class (secret level of the data accessed by the user (SP7)).

[0043] The authentication server terminal 3 executes the same operation of authentication as in the first embodiment. The authentication request unit 5D of the user terminal 5, having received the result of authentication informs the database retrieval application 5E of the result of authentication. The database retrieval application 5E, on the basis of the result of authentication, decides permission or inhibition of access to the highly secret

information in the local database 5C by the user (SP8). In this case, for example, the operation to user access such as displaying the secret information will be made. In such a configuration in which the user terminal 5 issues a request of authentication, the same effect as in the first embodiment may be obtained.

Embodiment 3

[0044] In Fig. 11 in which like reference numeral refer to like parts in Figs. 2 and 8, a procedure (SP2B, SP12A) is proposed in which a user rejects the authentication information acquisition S/W when the individual authentication information specified by the authentication information acquisition S/W 11 transferred from the authentication server 3 does not coincide with an user's intention (SP2B, SP12). The authentication server terminal 3 having suffered the rejection of acquisition selects another authentication information acquisition S/W again (SP20A). However, this is limited to the case where there is another authentication information acquisition S/W which can be selected again as described in connection to Fig. 4.

[0045] Where the biometrics is used as authentication information of an individual, it is necessary for a user to reject a specified biometrics acquisition device 6 involving dirtiness and unpleasantness. Specifically, although the biometrics is efficient to discriminate an individual from other persons, it gives rise to problems of privacy protection and sanitation as described above. For this reason, it is necessary for the user to reject or change the biometrics acquisition.

[0046] Where the biometrics acquisition device 6 is not trusted in security, the user may have an intention of specifying the other information than the biometrics, i.e. alternative means such as one-time password (OTP) even if it is complicate. In such a case, in accordance with the user's intention of rejection or changing, the authentication information acquisition S/W which dynamically acquires the information for authentication can be selected to identify an individual and decide the presence or absence of the access right of the individual according to the environment surely.

Embodiment 4

[0047] This embodiment, as means for obtaining the same effect as in the third embodiment, includes the mechanism of selecting the acquired authentication information in the authentication information acquisition S/W itself in the first and second embodiments. In the first embodiment, the authentication information S/W itself can select authentication D by both fingerprint and handwriting and that E by only the fingerprint. In this case, the authentication server transfers the authentication information acquisition S/W capable of acquiring both D and E.

[0048] The configuration and operation procedure in

the Web system 1 itself are the same as in the first and second embodiments. The displayed image of the authentication information acquisition S/W on the side of the user is shown in Fig. 12. The user selects either D or E to acquire authentication means and authentication information for himself. When he pushes either select button 12A or 12B, the authentication information acquisition S/W is operated to acquire the authentication information actually selected. The authentication server terminal 3 can decide the type of the received authentication information and if authentication can be made using a set of the received information. Thus, the same effect as in the third embodiment can be obtained.

[0049] In the first to fourth embodiments, the authentication information to be acquired has been determined by the authentication S/W. However, instead of this, the authentication information to be acquired may be only displayed on a screen. For example, at the number of times of authentication in the detailed database in the first embodiment, transfer of the fingerprint information and handwriting information is displayed on the screen. Thus, the user spontaneously operates the software for acquiring the authentication information in accordance with the displayed contents, and transfers the authentication information thus acquired to the authentication server terminal 3.

[0050] The transfer may not be concretely displayed, but previous transfer of the authentication information may be displayed. In this case, the user spontaneously operates the software for acquiring the authentication information to acquire all the items of information noticed previously from a manager in accordance with the user's memory and transfers the acquired authenticated information to the authentication server. In this way, the same effect as the first embodiment can be realized. In the above case of the previous transfer of the authentication information, which is not displayed concretely, the means for acquiring the authentication information is used in a fashion of a password. Therefore, security in acquisition of the authentication information can be improved remarkably.

[0051] In the first to fourth embodiments, the authentication of a user individual was made by the Web server terminal 4. The present invention, however, should not be limited to this, but may be widely applied to a general controller requires a user's individual such as an arrival/departure terminal device connected to a network.

[0052] As described above, in accordance with the present invention, when authentication should be made using the biometrics information, the authentication server freely selects and acquires the biometrics acquisition device and authentication information in accordance with the acquisition environment of the biometrics information by the user. Thus, a remote authentication system capable of identification of a user and decision of the presence or absence of the access right of the user can be surely realized.

[0053] If the authentication information designated is

not satisfactory for the user, he can change the authentication information to be acquired and reject its acquisition. Even when the biometrics acquisition device itself involves dirtiness and unpleasantness, or device for acquiring the biometrics information is not reliable, the identification of the user and decision of the presence or absence of the access right of the user can be made by an alternative means.

Claims

1. A remote authentication system having a network (2) which is connected to an authentication server (3), an authentication client (4) and a user terminal (5) for accessing data from the authentication client (4), in which authentication of the user accessing the authentication client (4) is made through the user terminal (5),
wherein said system comprises:

plural kinds of biometrics acquisition devices (7-10) connected to said user terminal (5); and plural authentication information acquisition softwares stored in said authentication server (3) according to the user terminal (5) and/or a user;

wherein in accordance with the operation of a prescribed authentication acquisition software corresponding to the user terminal (5), which is downloaded from the authentication server (3) in authentication, biometrics information acquired by one or plural kinds of biometrics acquisition devices and/or keyed-in user discrimination information are used, **characterized in that** said biometrics information and/or user discrimination information are selected depending on the secret level of the data to be accessed.

Patentansprüche

1. Fernbeglaubigungssystem mit einem Netzwerk (2), das mit einem Beglaubigungsserver (3) verbunden ist, einem Beglaubigungsklienten (4) und einem Benutzerendgerät (5) für den Zugriff von Daten von dem Beglaubigungsklienten (4), bei dem eine Beglaubigung des Benutzers, der zu dem Beglaubigungsklienten (4) zugreift, durch das Benutzerendgerät (5) erfolgt,
welches System aufweist:

mehrere Arten von Vorrichtungen (7-10) zur Gewinnung biometrischer Merkmale, die mit dem Benutzerendgerät (5) verbunden sind; und
mehrere Beglaubigungsinformations-Gewinnungssoftwarestücke, die in dem Beglaubigungsserver (3) gespeichert sind, entsprechend dem Benutzerendgerät (5) und/oder einem Benutzer;

nungsssoftwarestücke, die in dem Beglaubigungsserver (3) gespeichert sind, entsprechend dem Benutzerendgerät (5) und/oder einem Benutzer;

wobei gemäß der Operation einer vorgeschriebenen Beglaubigungsgewinnungs-Software entsprechend dem Benutzerendgerät (5), die von dem Beglaubigungsserver (3) bei der Beglaubigung heruntergeladen wird, biometrische Informationen, die von einer oder mehreren Arten von Vorrichtungen zur Gewinnung biometrischer Merkmale gewonnen wurden, und/oder eingegebene Benutzerunterscheidungsinformationen verwendet werden, **dadurch gekennzeichnet, dass** die biometrischen Informationen und/oder Benutzerunterscheidungsinformationen in Abhängigkeit von dem Geheimhaltungspegel der zuzugreifenden Daten ausgewählt werden.

Revendications

1. Système d'authentification distant ayant un réseau (2) qui est connecté à un serveur d'authentification (3), un client d'authentification (4) et un terminal d'utilisation (5) pour accéder à des données depuis le client d'authentification (4), dans lequel l'authentification de l'utilisateur accédant un client d'authentification (4) est réalisée à travers le terminal d'utilisateur (5),
dans lequel ledit système comprend :

plusieurs types de dispositifs (7-10) d'acquisition de biométrie, connectés audit terminal d'utilisateur (5) ; et une pluralité de programmes d'acquisition d'informations d'authentification, stockés dans ledit serveur d'authentification (3) selon le terminal d'utilisateur (5) et/ou un utilisateur ;

dans lequel, conformément au fonctionnement d'un programme d'acquisition d'authentification prescrit selon le terminal d'utilisateur (5) qui est téléchargé depuis le serveur d'authentification (3) dans l'authentification des informations de biométrie acquises par un ou plusieurs types de dispositifs d'acquisition de biométrie et/ou des informations de discrimination d'utilisateur saisi au clavier sont utilisées, **caractérisé en ce que** lesdites informations de biométrie et/ou lesdites informations de discrimination d'utilisateur sont sélectionnées en fonction du niveau de secret des données devant être accédées.

FIG. 1

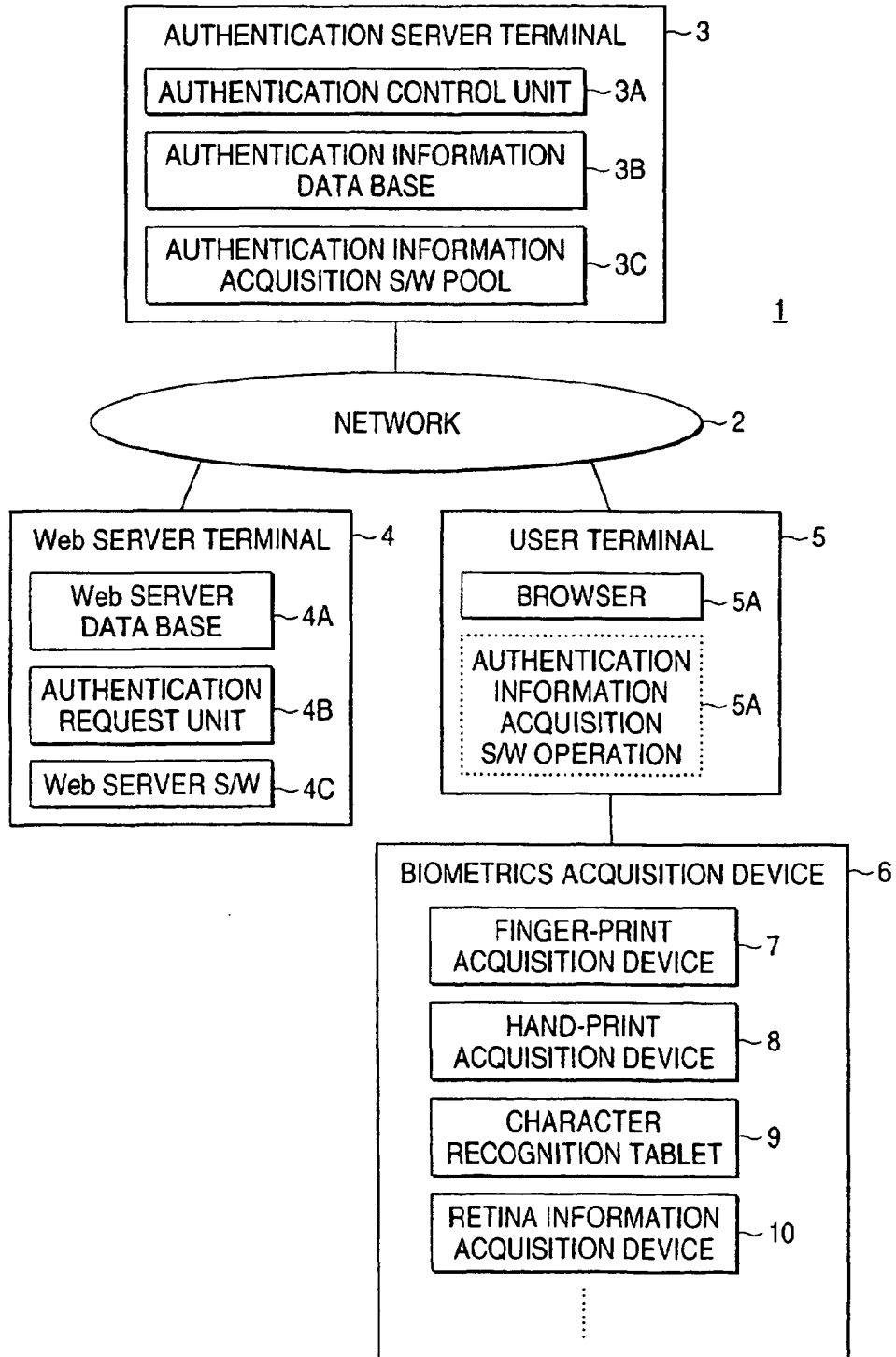


FIG. 2

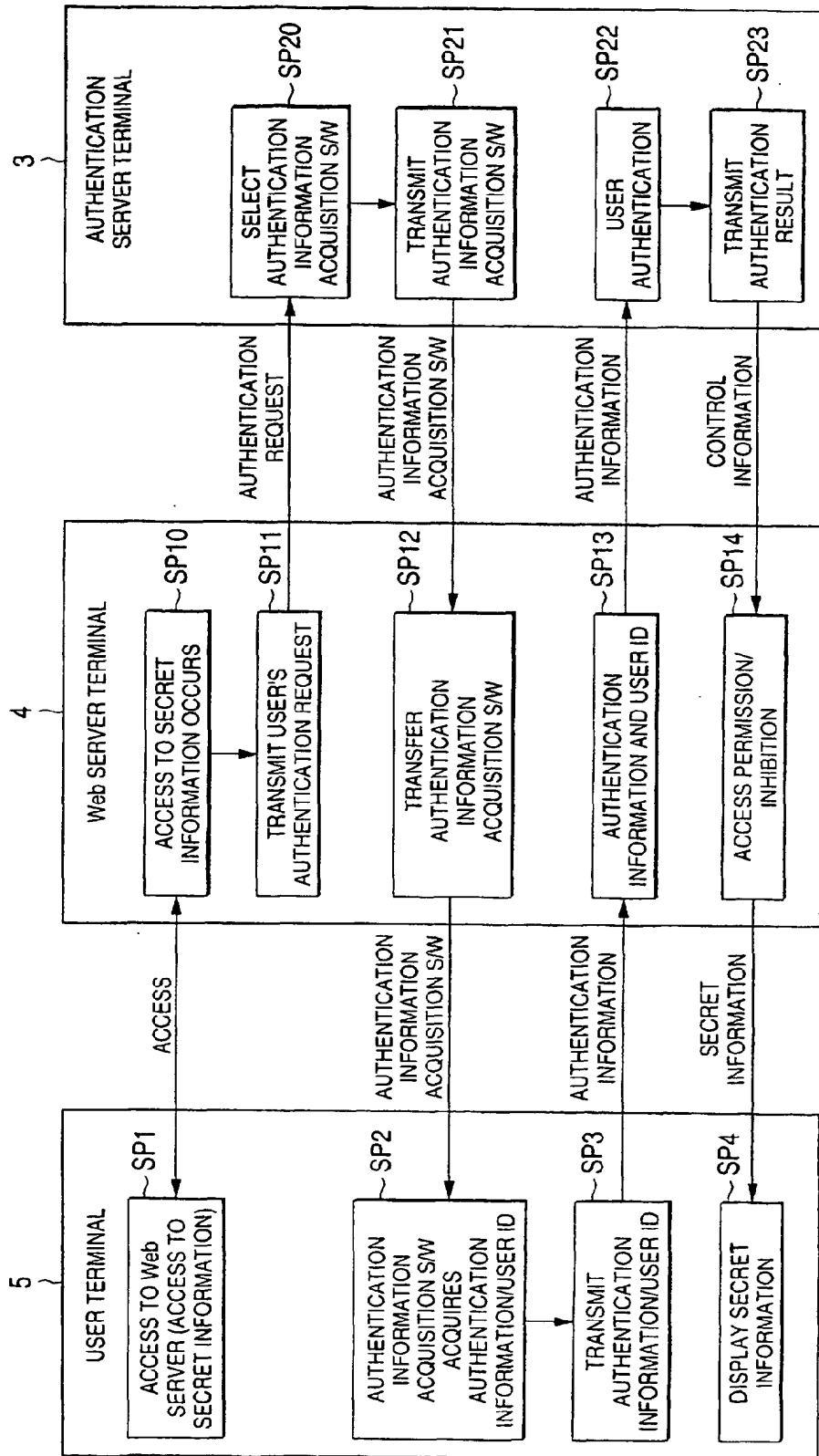


FIG. 3

USER ID	1 {NAME, FIRM, MEMBER NUMBER, BELONGING, ADDRESS, TELEPHONE NO., ETC.}	2
USER LEVEL	2			
AUTHENTICATION INFORMATION	{FINGERPRINT 1, FINGER PRINT 2, HANDWRITING, RETINA, PASSWORD, ONE-TIME PASSWORD INFORMATION}			

FIG. 4

LEVEL	DATA CLASS	AUTHENTICATION INFORMATION ACQUISITION S/W
1 (HIGHEST SECRET)	1 ~ 10	A, B, C
2	11 ~ 20	D, E, F
3	21 ~ 30	G, H

A: FINGERPRINT AND RETINA
 B: FINGERPRINT TWO FINGERS
 C: RETINA AND HANDWRITING
 D: FINGERPRINT AND HANDWRITING
 E: FINGERPRINT
 F: HANDWRITING
 G: ONE-TIME PASSWORD
 H: PASSWORD

FIG. 5

AUTHENTICATION CLIENT ID	AUTHENTICATION INFORMATION ACQUISITION S/W
	E, F
15	C, D, E
	A, B, C
	D, E, F
	G, H

FIG. 6

APPLICATION ID	AUTHENTICATION INFORMATION ACQUISITION S/W
	C, E, G
25	A, D, E, F
	E, F
	G, H

FIG. 7

USER ID	1 {NAME, FIRM, MEMBER NUMBER, BELONGING, ADDRESS, TELEPHONE NO., ETC.}	2
USER CLASS	GENERAL			
USER LEVEL	2			
USABLE CLIENT ID	10, 15			
USABLE APPLICATION ID	8, 25, 36			
APPLICATION CONTROL INFORMATION	Key-1			
AUTHENTICATION INFORMATION	{FINGERPRINT 1, FINGERPRINT 2, HANDWRITING, RETINA, PASSWORD, ONE-TIME PASSWORD INFORMATION}			
CHECKING LOG	LAST TIME: AUTHENTICATION INFORMATION ACQUISITION S/W E SELECTION, CHECKING EVALUATION 90%, FINGERPRINT 1 = 90% BEFORE LAST TIME: AUTHENTICATION INFORMATION ACQUISITION S/W D SELECTION, CHECKING EVALUATION 75%, FINGERPRINT 2 = 80%, HANDWRITING = 70% ...			
TOTAL NUMBER OF TIMES OF AUTHENTICATION	20			
SELECTION CONDITION	TOTAL NUMBER OF TIMES OF AUTHENTICATION (OTHER EXAMPLE: CHECKING RATE)			

FIG. 8

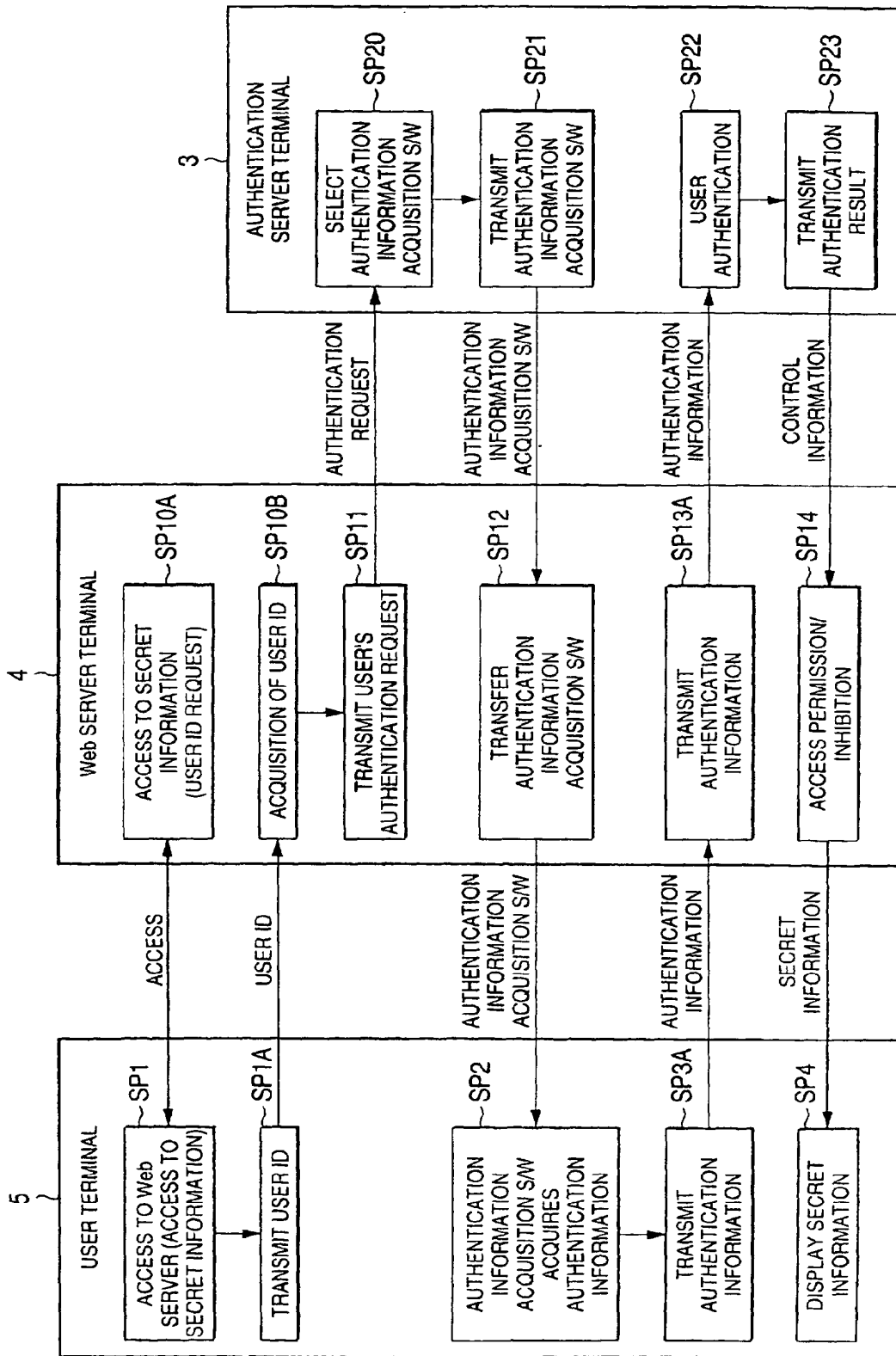


FIG. 9

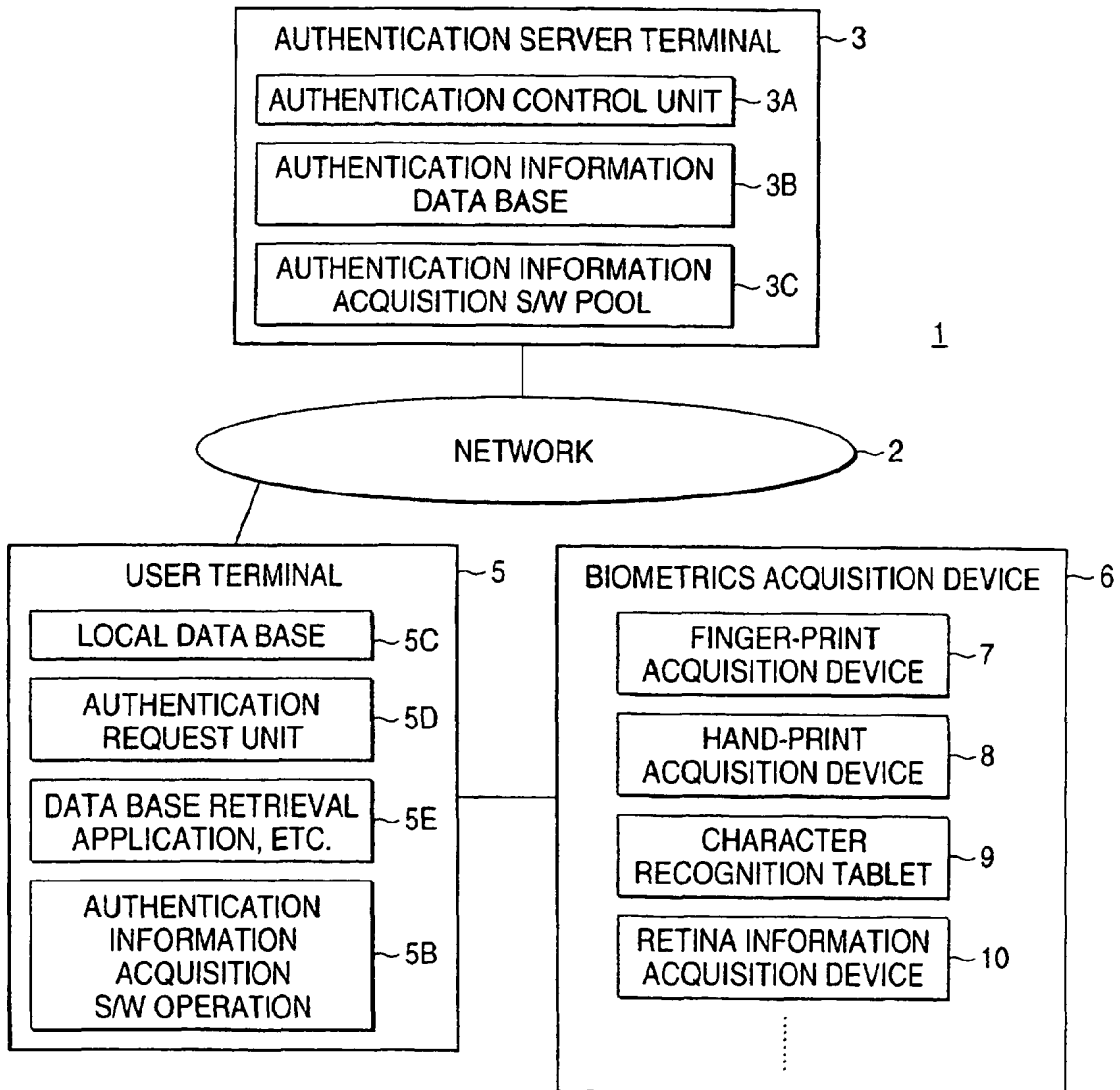


FIG. 10

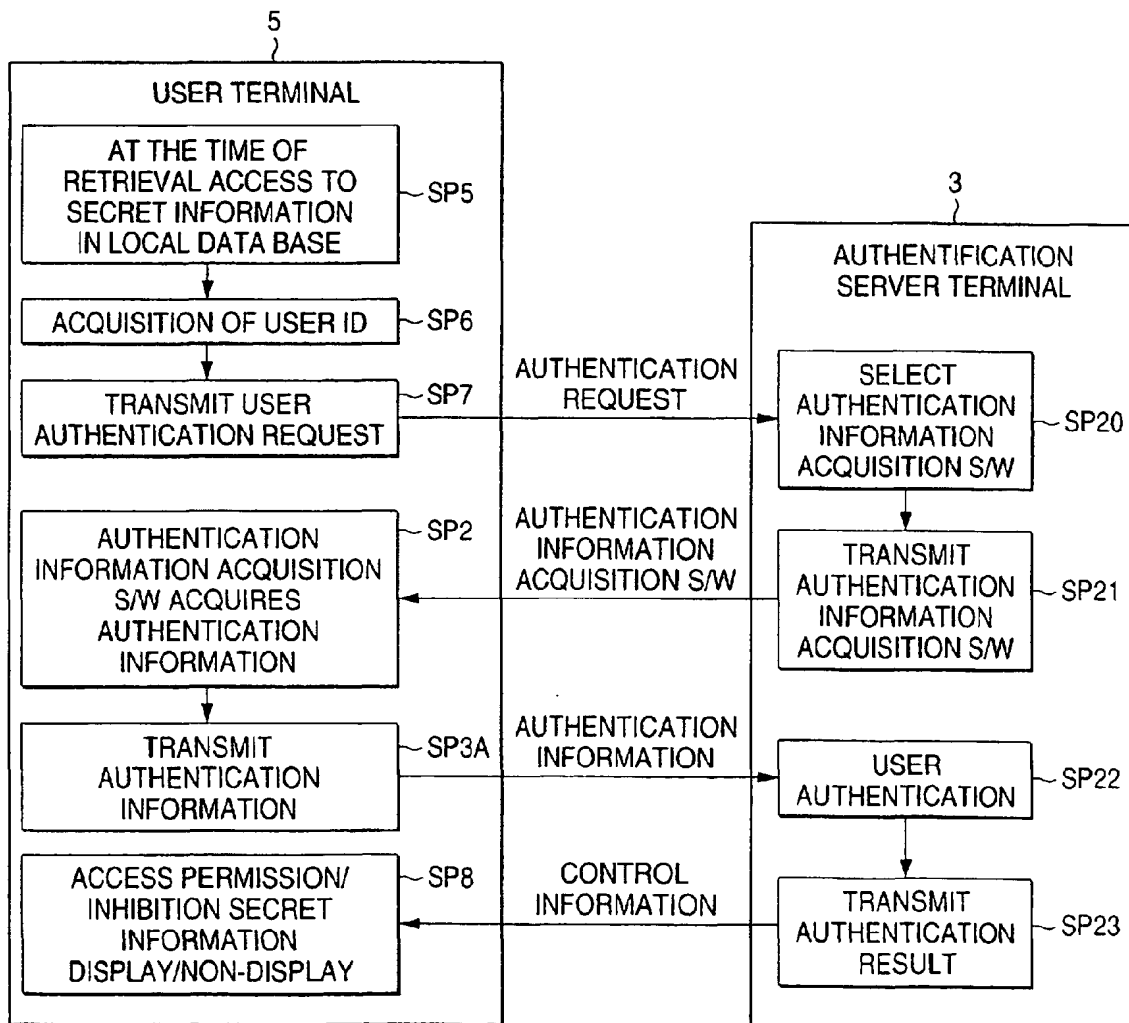


FIG. 11

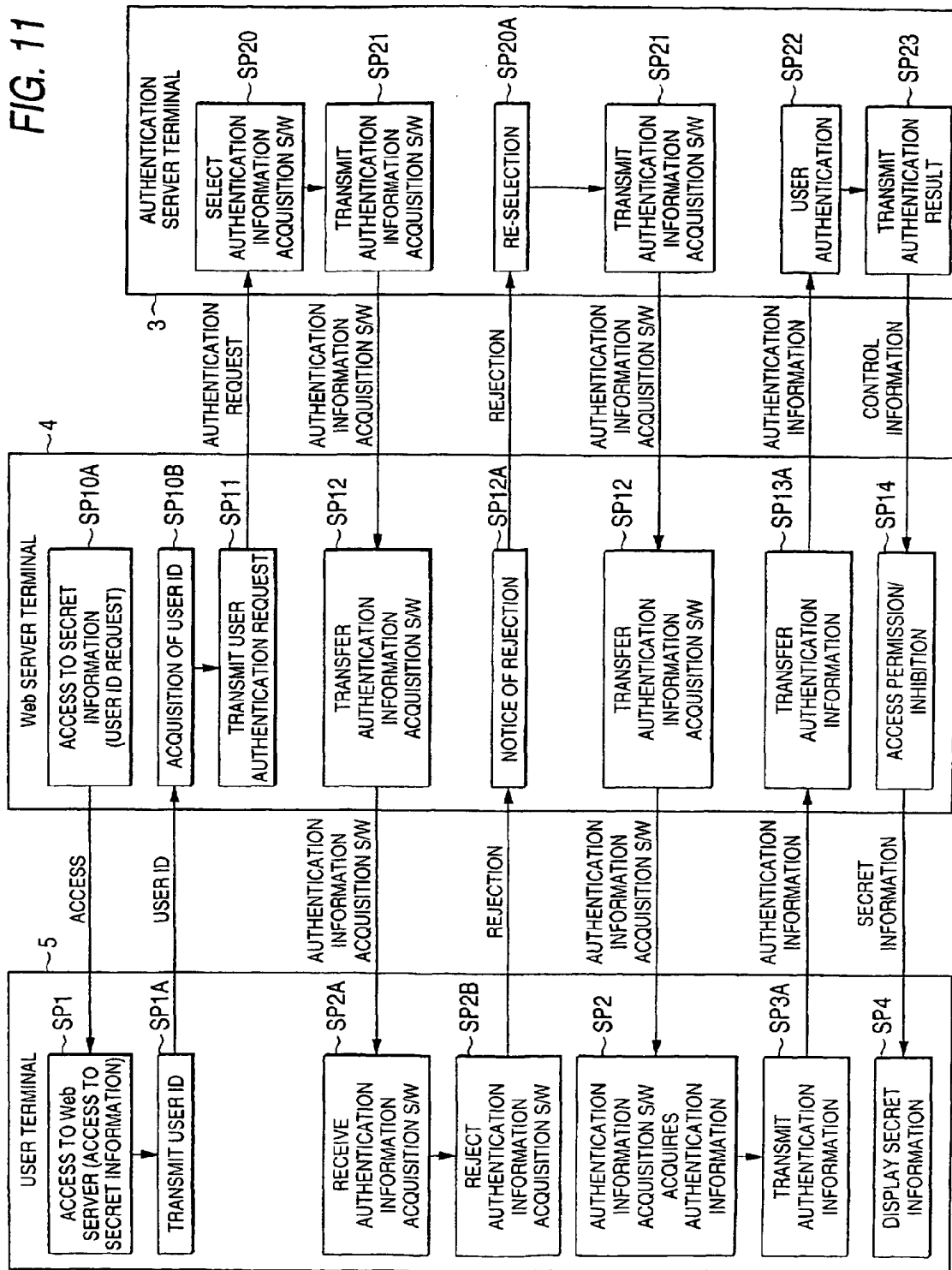


FIG. 12

